

WHAT IS CLAIMED IS:

1. A method for intrusion detection of network traffic comprising:

storing a data file comprising data defining one or more signature definition and one or more parameters and associated values;

generating, for each of the one or more signature definitions, an inspector instance based on the data file; and

executing, for each of the one or more signature definitions, the generated inspector instance to detect network traffic matching the signature definition.

2. The method of Claim 1, and further comprising:

storing a user data file comprising signature definitions, each modified signature definition comprising a signature identifier associating the modified signature definition with a corresponding signature definition stored in the data file; and

generating, for each of the modified signature definitions, a revised inspector instance based on the modified signature definition and the corresponding generated inspector instance.

51

3. The method of Claim 1, wherein the data file comprises, for each signature definition, data comprising:

a signature identification number parameter and  
5 associated value;

a signature name and associated string; and

one or more parameters and respective values  
defining characteristics of the signature.

10 4. The method of Claim 1, wherein each signature definition is stored in a separate line of the data file.

5. The method of Claim 2, wherein the one or more  
modified signature definitions comprises modified values  
15 for associated modified parameters and no values  
indicative of the parameters in the corresponding  
signature definition that are not modified.

6. The method of Claim 1, wherein the data file  
20 comprises a file received from a sensor provider.

7. The method of Claim 1, wherein the data file  
comprises a file generated by a user.

25 8. The method of Claim 1, wherein receiving the data file comprises receiving the data file at a sensor configuration handler.

9. The method of Claim 1, and further comprising  
30 receiving configuration data from a user and storing the received configuration data in a user data file.

10. The method of Claim 1, and further comprising:
- storing a user data file comprising one or more user-defined signature definitions, each user-defined
- 5 signature definition comprising a signature identifier not associated with any of the signature definitions in the data file; and
- generating, for each of the user-defined signature definitions, an inspector instance based on the user-
- 10 defined signature.

0990860-110901

11. A method for use in intrusion detection comprising:

storing a default signature file defining one or more default signatures;

5 storing a customized signature file defining one or more custom signatures;

10 automatically generating, for each of the one or more signatures defined in the default signature file, executable code operable to detect intrusions associated with the default signature; and

automatically generating, for each of the custom signatures, executable code operable to detect intrusions associated with the custom signature.

15 12. The method of Claim 10, wherein storing a customized signature file comprises storing modifications of one or more of the default signatures.

20 13. The method of Claim 10, wherein automatically generating, for each of the one or more custom signatures comprises automatically generating, for each custom signature, executable code operable to detect intrusions associated with the custom signature based on the generated executable code of an associated default  
25 signature.

14. The method of Claim 11, wherein the one or more custom signatures comprises modifications of the default signatures.

15. The method of Claim 11, wherein generating, for each of the one or more default signatures, comprises generating executable code associated with the default signature based on an inspector shell.

5

16. The method of Claim 15, wherein the executable code associated with the default signature is operable to compare a plurality of parameter values to a plurality of parameter values defined by the default signature.

10

17. The method of Claim 11, wherein the default signature file comprises, for each default signature;

a signature identification number parameter and associated value;

15

a signature name and associated string; and  
one or more parameters and respective values  
defining characteristics of the default signature.

18. The method of Claim 11, wherein the custom signature file comprises, for each signature:

a signature identification number parameter and associated value;

a signature name and associated string; and  
one or more parameters and respective values  
defining characteristics of the default signature.

25

19. A method for use in intrusion detection comprising:

providing a sensor having a plurality of defined signatures;

5 communicating to the sensor a desire to create a modified signature from a signature to be modified;

receiving from the sensor data indicative of parameters and associated values for the signature to be modified; and

10 providing to the sensor a modified value for at least one of the parameters to create a modified signature.

20. The method of Claim 19, and further comprising  
15 storing data associated with the modified signature in the sensor at a location separate from the associated unmodified signature.

21. The method of Claim 20, and further comprising  
20 storing in the sensor the name, signature identification number, and one or more parameters and associated values for only the modified values for the modified signature.

22. The method of Claim 19, and further comprising  
25 communicating to the sensor the name of an engine associated with the signature to be modified.

23. The method of Claim 20, wherein storing data associated with the modified signature comprises storing  
30 a plurality of parameter names and associated values.

24. The method of Claim 19, and further comprising selecting a signature to be modified from the plurality of defined signatures.

5           25. The method of Claim 22, and further comprising  
receiving a list indicative of all defined signatures  
associated with the engine.

26. The method of Claim 19, wherein providing a  
10 sensor having a plurality of defined signatures comprises  
providing a sensor having a default data file defining  
the defined signatures.

27. The method of Claim 26, and further comprising  
15 updating the default file.

28. A system for intrusion detection comprising:  
a sensor for detecting possible network intrusions,  
the sensor comprising:

- 5           one or more engine groups each associated with  
one or more network detection engines; and  
a configuration handler comprising:  
a default signature file storing one or  
more signature definitions defining one or more  
10       respective default signatures for use by the  
sensor; and  
a user signature file storing a plurality  
of user-defined signatures for use by the  
sensor; and  
15       wherein each network detection engine is  
operable to generate an executable code based on  
either one of the stored default signatures or one  
of the stored user-defined signatures, the  
executable code operable to detect a network  
20       intrusion defined by the associated user-defined  
signature or the associated default signature.

29. The system of Claim 28, wherein the  
configuration handler further comprising stored  
25       modifications to the default signatures.

30. The system of Claim 29, wherein the stored  
modifications are stored in the user signature file.

31. The system of Claim 28, wherein the configuration handler further comprises a user interface operable to:

5 receive an identification of a signature to be modified;

provide a list of parameters and associated values for the signature to be modified;

receive revised values for one or more of the parameters; and

10 write a revised signature to the user-defined data file.

32. The system of Claim 28, wherein the configuration handler further comprises a user interface operable to:

15 provide a list of possible parameters for a particular engine;

receive a plurality of values for one or more of the parameters to define a user-defined signature associated with the engine; and parameters; and

20 write a user-defined signature to the user signature file.

33. The system of Claim 28, wherein the configuration handler further comprises a reader and dispatcher operable to read data from the default signature file and user signature file and transmit the read data to the one or more engine groups.

34. The system of Claim 28, and further comprising  
a management console associated with the sensor and  
operable to communicate configuration data to the  
configuration handler and receive configuration help  
5 information from the configuration handler.

00000000-110001  
10000000-00000000



36. A method for use in intrusion detection of network traffic comprising:

storing in a memory a signature definition  
5 associated with a signature to be detected, the signature definitions comprising:

an identifier for the signature; and  
one or more parameter-value pairs associated  
with the signature, each parameter-value pair  
10 comprising a parameter name and associated parameter value; and  
determining, based on the signature definition, the values that associated parameters of network traffic must take to meet the signature.

15 37. The method of Claim 36, and further comprising storing a plurality of signature definitions in a data file, each signature definition on a different line of the data file.

20 38. The method of Claim 36, wherein each signature definition further comprises an engine parameter and an associated name for the engine parameter.

25 39. The method of Claim 36, wherein each signature definition further comprises an identification parameter preceding the signature identifier.